INTERNET, CITIZENS, AND PUBLIC ORGANIZATIONS: THE POWER OF SERVICE PROVIDERS IN FOSTERING OR HAMPERING TRANSPARENCY

Tommaso Federici and Alessio Maria Braccini
Department of Economics and Business (DEIM), University of Tuscia, Viterbo, Italy
Centro di Ricerca sui Sistemi Informativi (CeRSI), Luigi Guido Carli University, Rome, Italy

ABSTRACT
The continuous evolution and the growth of the Internet made it a globally diffused and accessible network were users are not only content consumers, but also content providers. The possibility of diffusing data and information, from official sources and often intended to be kept confidential or restricted, can promote the transparency in the communication process of public organizations with citizens. At the same time other subjects not directly involved in the process of information diffusion, like the service providers, are in the position to promote or hamper this phenomenon. Within these boundaries this paper uses agency theory to investigate the case of WikiLeaks, an international non profit organization that gained widespread global attention for the diffusion of documents unveiling the activities of the US diplomacy.

KEYWORDS
Internet, WikiLeaks, Transparency, E-participation, Agency Theory

1. INTRODUCTION

The Internet is continuously growing. The number of users accessing the network has grown to 2 billion, with a penetration rate of 30.2% of the world population and a growth rate of 480.4% over ten years (InternetWorldStats, 2011). The growth in size and the evolution in terms of capabilities, content and services offered, saw the role of Internet user changing. Due to the diffusion of blogs, forums, chats, social networks, and web 2.0 technologies, today's Internet user has the possibility to both consume as well as produce and share data and information using a plethora of different interactive tools, with the intent to entertain, contribute, and participate.

In a recent paper (Federici & Braccini, 2012) we argue that this new landscape could modify the way the communication of an organization with its stakeholders is performed. We assert that citizens could put more pressure on public administrations and governments, thanks to the increased transparency due to the greater availability of official data and information (not only comments or opinions) on their work at a low cost. We also maintain that the specific subjects who were not previously involved in the communication process between public organizations and citizens, or who were playing a marginal role, could now have more power. We mainly refer to the fact that data intended to be confidential can be revealed, or incomplete data can be completed and integrated or confuted by similar data shared by Internet users.

The relationship between transparency and government as a solution to reduce corruption and improve accountability has already received attention (Gant, Gant, & Johnson, 2002; Kaufman & Bellver, 2005). Rich and clear information can improve the quality of the society, as more informed citizens demand to be better governed and governments are positively influenced by such pressure (Islam, 2003).

In this scenario, rather than having few central points from which data and information are broadcasted, several independent and unofficial agents cooperate and compete in a multicast fashion to share data and information. This phenomenon already provoked some results, as in the case of the Fukushima nuclear crisis where citizens assumed the role of data providers in absence of official data on radiation levels (Federici &
Braccini, 2012), and might require a change in the management styles in the communications between an organization and its stakeholders.

However not all actors involved in this landscape are aware of this phenomenon. At the same time, many constraints and hurdles could potentially impede the change in progress, as for example:

- information difficult to be used, because of foreign language, competence needed, huge quantity, or even inadequate technology development (Spagnoletti & Resca, 2012);
- behavior of media operators which may choose if, what, and when to publish;
- service operators which may close servers, connections, bank accounts of the subjects who expose information.

As such, we believe this to be an interesting research topic to investigate.

The objective of this paper is to investigate the specific phenomenon of the service providers’ impact on the increased transparency fostered by the diffusion of data and information on the Internet, allowing citizens to be informed on specific decisions made and actions taken by public administrations and governments. In particular, we focus on the role and the power that such newcomer actors might have in the above mentioned landscape and develop a taxonomy about such subjects. The structure of the paper is as follows: section 2 will provide some information regarding the methodological questions as well as the theory adopted to investigate the case. The case will be described in section 3 and later discussed in section 4. Some final remarks will conclude the paper in section 5.

2. RESEARCH DESIGN AND THEORETICAL FRAMEWORK

In the scenario described in the introduction, this paper aims at investigating the importance and the power of service providers in promoting or hampering the capability of specific subjects to broadcast information capable of increasing the transparency in the communication process between public organizations and citizens.

Following the research agenda proposed by Federici & Braccini (2012), we are interested in investigating the power potentially wielded by specific subjects, the providers of support services, in the process of information diffusion. We relied on the theoretical contributions pertinent to agency theory to investigate actions and decision made by the subjects involved in our case.

The agency theory describes the principal-agent relationship and was proposed to explain the hostile relationship between the management and the ownership of enterprises (Eisenhardt, 1989; Hung, 1998). Such theory can anyhow be applied in other context were two different subjects occupy the positions, respectively, of principal and agent. More generally agency theory can be applied to cooperation relationships where the parties involved have different goals and division of labor (Jensen & Meckling, 1976). Sometimes this difference in terms of goals and division of labor foster conflicts and turns the relationships between the two parties in a hostile one.

In the kind of relationships where agency theory is applied, one part (the principal) delegates a piece of work to another part (the agent). The latter performs the work that has been assigned (Eisenhardt, 1989). The relationship between the principal and the agent is seen by the agency theory with the eyes of a contract. Agency theory thus describes the interactive relationships amongst several subjects playing the role of agents and principals with a network of contracts.

In principal-agent relationships two problems might emerge: the agency problem, and the risk-sharing problem. The agency problem arises when there is a conflict between the goals desired by the principal and the agent, and when it is difficult for the principal to verify what the agent is actually doing (Eisenhardt, 1989). The risk-sharing problem arises when the principal and the agent have different attitudes toward risk, and might therefore prefer different actions as a consequence to their different risk preferences.

Under a methodological point of view, we followed Yin’s single case study methodology (Yin, 1994). In this paper we focus on the case of WikiLeak, an international non profit organization that gained significant international attention after releasing several documents containing confidential information on the work of USA diplomacy. The data for the cases were gathered from a mix of different sources: international newspapers, official and private websites, blogs. We mainly paid attention to the sequence of multiple actions and reactions seen in this case.
WikiLeaks is a useful example of how the Internet fosters transparency in the communication process between citizens and public organizations (Federici & Braccini, 2012). The rationale justifying the selection of this case consists in the possibility to observe the phenomenon in its wholeness. Since the event we are referring in this paper (described in the following section), is dated November 2010, we were in the position to observe not only the phenomenon but also the consequences in terms of decisions and actions taken by all the subjects involved. This circumstance does not hold true for other similar events that are contemporary.

3. CASE DESCRIPTION

3.1 WikiLeaks: Description of the Context

WikiLeaks is an international non profit organization that publishes on its website documents received from anonymous sources. The documents received and published are usually not intended to be disclosed, and are thence declared by the originally owning organizations as classified or confidential. Its content is related to activities performed by government or large companies. WikiLeaks publishes original material (i.e. documents, footage, pictures) not users comments or opinions. WikiLeaks, thanks to the usage of Internet and cryptography technologies, warrants the anonymity of the whistleblower or of the source that provides the document. Prior to the publication, WikiLeaks checks originality and reliability of the documents received.

The website of WikiLeaks was launched in 2006 with the goal to bring important news and information to the public, and to safeguard whistleblowers and contributors security, protecting them against possible reprimals for having disclosed classified documents. The website was originally started as a wiki, where users could edit content and post comments. Soon after, the website moved to a more traditional publication model and no longer accepted users contributions. Therefore notwithstanding its name, WikiLeaks is currently no longer a wiki. The WikiLeaks website size grew to more than 1 million documents on its database one year after the start of its activities. The Internet activist Julian Assange is the founder and the main actor behind WikiLeaks activity.

In recent years WikiLeaks released a number of documents that frequently became front-page news items. WikiLeaks contributed to share documents regarding events of the war in Afghanistan or Iraq, and on political activities in African countries like Somalia or Kenya.

3.2 The "Cablegate" Case

More recently, the focus on WikiLeaks was due to the so-called “Cablegate”. On November 2010 WikiLeaks announced a future disclosure of a significant amount of documents. Following this announcement, media speculated that they might contain diplomatic cables. WikiLeaks indeed released in many forms part of 251.287 classified documents containing confidential information on the work and activities of US diplomacy around the world covering the period from 1966 to 2010. Such documents were disseminated to news operators like the daily El Pais, Le Monde, The Guardian, The New York Times, and the weekly Der Spiegel. WikiLeaks, through the voice of Julian Assange’s lawyer, tried to receive information from people who could be placed at significant risk by the cable release prior massive disclosure of the cables. However the US Department of State refused to engage in a negotiation regarding release or dissemination of illegally obtained US Government classified materials (Koh, 2010).

The content of the cables disclosed, which were confidential but not top-secret, were related to critiques and appraisals of the policies of the hosting countries of various US embassies, for example: the political maneuvers regarding climate change, tension in the Middle East, the war on terror, assessment of various threats around the world, and other diplomatic activities. A first release of these documents, covering only a portion (220) of all the cables in possession of WikiLeaks, was uploaded online on November 28th by The Guardian newspaper in the UK. Reactions from involved parties (mainly the US government but also the leaders of the most prominent western democracies) were a mixture of strong criticism, commendation, bewilderment, dismay, and quiescence.
3.3 Reactions by Government and Impediments by Service Providers

The US Secretary of State described the leaks as an attack on America’s foreign policy and an attack on the international community, the alliances and partnerships, the conventions and negotiations that safeguard global security and advance economic prosperity.

Legal actions were also taken against WikiLeaks by the US government soon after the cables release, as well as pressure on WikiLeaks itself from US congressmen or senators, and also on other organizations supporting with their services its activity (i.e. service providers like Amazon, PayPal, and MasterCard). The Chairman of the US Senate Homeland Security and Government Affairs Committee and his staff threatened service providers with prosecution for violation of the Espionage Act, as it had already happened to WikiLeaks, if they would have not halted their services' provision in favor of it (O’Leary, 2010). With the abovementioned communication, the US Department of State informed WikiLeaks that the only fact that WikiLeaks was in possess of those documents was a violation of laws. With the same notice the US Department of State blocked any possible attempt of negotiation to prevent publication.

There were other reactions, in terms of attacks directed to the WikiLeaks website and its founder Julian Assange. At the end of November 2010 WikiLeaks declared that its website was undergoing a massive distributed denial of service attack. Soon after in December 2010, EveryDNS.net, the DNS service provider of WikiLeaks, aborted its DNS service for the WikiLeaks website. Connections to the WikiLeaks website were no longer possible after this date. Right after EveryDNS.net, Amazon.com also revoked its services depriving the WikiLeaks website of the necessary hosting provision. The website was then necessarily migrated to another service provider and a mass-mirror campaign of the WikiLeaks website was later started.

A Twitter account was also set up to share documents on several multiple websites like wildfire, impeding future distributed denial of service attack. As a consequence, the US Justice Department sued Twitter formally asking to communicate the details of the users accounts that had been associated with WikiLeaks (Repubblica, 2011). Twitter answered to this request by only informing its users of this request.

In addition to the legal and technical aspect the WikiLeaks website also faced a global financial blockade by major finance companies who were supporting its activity. WikiLeaks had indeed been counting on users donations to support its activity since the website publication. Financial intermediaries were then necessary to collect these donations. At first Moneybookers, an e-commerce provider, which collected donations for WikiLeaks, announced in October 2010 that it would have proceeded in order to evaluate the compliance of its relationship with WikiLeaks through an investigation on money laundering, conducted by government authorities.

On December 2010 the Bank of America announced it would have not processed any transaction of any type related to WikiLeaks. The Bank of America argument was that WikiLeaks was engaged in activities against the Bank of America internal policies for processing payments. The Bank of America also addressed lawyers to put a stop to WikiLeaks activity.

Still on December 2010, PayPal, the Internet payment providing service owned by eBay, closed down the account of a foundation that had been redirecting donations to WikiLeaks. PayPal mentioned the violation of its Acceptable Use Policy by the foundation specifically pointing out that the account was used for activities that could encourage other people to engage in illegal activities.

After eBay, on December 6th the Swiss bank PostFinance announced it had frozen the assets of Assange stating that he had provided false information regarding his place of residence when opening the account. On the same day, MasterCard announced action to prevent WikiLeaks from accepting MasterCard branded products stating that MasterCard rules prohibit customers from directly or indirectly engaging in or facilitating any illegal activity. The day after, Visa announced to suspend payments to WikiLeaks. Media also reported that Apple had removed on December 21st an application from is App Store which provided access to the released cables.

Partial financial support to WikiLeaks came from XIPWIRE and The Guardian newspaper, who announced two new ways to donate money to WikiLeaks. Datacell, a Swiss-based IT company that enabled WikiLeaks to accept credit card donations, took legal action against Visa and MasterCard to resume their payment services to the website. Datacell also filed a complaint against Visa and MasterCard for infringement of European antitrust rules claiming the stopping of the contracts with WikiLeaks violated the competition rules of the European Community. A UN High Commissioner for Human Rights also claimed
that Visa, MasterCard, and Amazon could have violated WikiLeaks’ right to freedom of expression by ending their service contracts.

Notwithstanding the support provided by these latter companies, on October 2011 Assange declared that the financial blockade had destroyed more than 90% of WikiLeaks’ revenue. WikiLeaks activity was then suspended to fight the blockade and raise new funds (Addley & Deans, 2011).

4. DISCUSSION

By reading the case description, a plethora of actors appear on the same scene: a website devoted to the publication of information otherwise hidden, WikiLeaks, great international newspapers such as El Pais, Le Monde, The Guardian, Der Spiegel, The New York Times, and some very different service providers, like EveryDNS.net (a Domain Name Services maintainer, presently retired), Twitter (a social network), Amazon.com (an electronic shop, but also a hosting provider like in this case), Moneybookers (an e-commerce provider), Bank of America (a banking company), PayPal (a payment service provider, owned by eBay which made the relative decisions), PostFinance (a Swiss bank specialized in electronic account management), MasterCard and Visa (both electronic payment companies), Apple (an IT producer, which in this case hosted a software useful to benefit of WikiLeaks), XIPWIRE (a mobile payment service provider), and DataCell (a host provider).

However except for the newspapers and WikiLeaks, all the other subjects are unexpected players in the information domain. Most of us, as regards political or social information, think only to the media operator who actually publishes it, like WikiLeaks in the "Cablegate" case. Yet, we can observe in such case a higher number of other subjects not directly involved in media sector, with their maybe surprisingly relevant role. Moreover the newspapers have a partially different role in the scenario of multicasted information; this theme is anyhow out of the scope of this paper, which is focused on the role and behavior of the subjects we have called "service providers".

Actors not directly involved in information diffusion exist even in traditional channels, like press or radio and TV broadcasting, providing services to media operators. However when considering information spread in new ways by new subjects through new channels like the Internet, we observe that the role of such "hidden" actors becomes more evident and their power increases, as in the WikiLeaks event.

| Table 1. Taxonomy of service providers in information multicasting on the Internet. |
|---------------------------------|---------------------------------|---------------------------------|
| **Group**                      | **Services provided**           | **Examples of provider**        |
| 1. Financial operators         | Remote accounting management   | Moneybookers                    |
|                                | Payments                        | Bank of America                 |
|                                | Donations collection            | PayPal                          |
|                                | Etc.                            | PostFinance                     |
|                                |                                 | MasterCard                      |
|                                |                                 | Visa                            |
|                                |                                 | XIPWIRE                         |
| 2. Technical services providers| Information management         | EveryDNS.net                    |
|                                | Communication through the web   | Amazon.com                      |
|                                | Data hosting                    | Apple                           |
|                                | IP addresses management        | DataCell                        |
|                                | Etc.                            |                                 |
| 3. Social networks             | Continuous communication among team members and supporters | Twitter                         |

We can classify the subjects encountered in the "Cablegate" case, with the exception of the media operator, in three groups, drawing a taxonomy of the service providers engaged in supporting a subject who promotes transparency through the Internet (see table 1):

The first group (the largest in this case) is that of financial operators, which provide services like: remote accounting management, payments, donations collection, etc.;
The second one is that of technical service providers, which also are essential in information management and communication through the web, as they host data, manage IP addresses and so on. Finally, the third group in this case consists of only Twitter which, being a social network, gives the chance of continuously communicating with team members, supporters etc.

When trying to interpret the behaviors of the service providers in the "Cablegate" case through the lens of the agency theory (Eisenhardt, 1989), we first have to identify who is the principal and who the agent. We consider WikiLeaks as the principal in question, as it delegated pieces of work to other subjects in order to extend its capacity and to better achieve its main purpose. Each of the service providers played respectively and separately, the role of agent in front of the same principal (WikiLeaks), as each of them was in charge of a segment of activity assigned to it by the principal.

In the presented case none of the agents have a direct involvement (nor a visible interest) in the process of data and information diffusion, which instead is the declared aim of the principal. All the agents have as their own mission the provision of one or more services, possibly making money thanks to that. The subjects at the two sides of each relationship, namely WikiLeaks and a service provider, do not then share the same aim, point of view, interest, mission.

Principal and agents were linked in this case by signed contracts, with specifications of the service to be provided, and of the service conditions, price, liability etc. Like in any similar case, the principal (the subject who commits an activity to someone else) feels reasonably sure that, as long as it pays regularly the fees and respects license agreements, it should count on the service hired, at least until the contract expiry. Even though in the common world, the principal and the agent may not share the same vision of the world, goals or field of interest, such divergences do not cause problems and each side of the relationship keeps to take benefit of it.

In the discussed case, most of the agents are instead both out of the group of financial operators (Moneybookers, Bank of America, PayPal, PostFinance, MasterCard, Visa) and of the technical service providers (EveryDNS.net, Amazon.com, Apple) that decided to interrupt the services provision to WikiLeaks, not because a missed payment or other ascertained violation of the conditions by it (O’Leary, 2010). On the contrary, as mentioned above, a UN High Commissioner claimed some of these subjects, after having interrupted their service, for their violation of the contract terms they made in damn of WikiLeaks.

The only exceptions were Twitter, which resisted to strong pressure, and other smaller service providers, like Datasell and XIPWIRE. Their behavior however did not save WikiLeaks from having to face problems with fund raising and data management, which halted its activities.

Agency theory is useful to interpret the behaviors of all the subjects in question. The goals of the principal and of the agents were already different in the past, but this had not cause any problem before the announcement of the disclosure of a huge amount of US diplomatic cables. The risks possibly coming out of the provision of some services to WikiLeaks were not formerly perceived as high or compromising. Once such documents were disclosed, the US Government’s reaction together with some explicit threats by some influential US politicians (O’Leary, 2010), to prosecute any service provider as well as WikiLeaks, altered profoundly the perception of the risk for the agents.

Here we can see a situation where goals are different for the principal and the agent, and the principal promotes an action to achieve an important goal for itself but not relevant for the agent. At the same time there is an increased risk for both the subjects. This can change the agent's perception of the relationship, possibly causing hostility between the two sides and even the interruption of the relationship, particularly if it is defined by a contract. Thus the principal's goal may then not be partially or fully achieved, because of the behavior of the agent, who is in charge of a support but essential activity.

In the WikiLeaks case, the key issue is that it concerns the critical process of information diffusion, which as previously discussed feeds transparency, a crucial condition to improve government. As observed in this case, pressuring support service providers, even when the final publisher resists to pressures, can block the diffusion of information.

When considering the "Cablegate" case, what must be noted is that pressure was exerted not only on WikiLeaks but also on its service providers, which soon capitulated. By contrast, traditional media operators like the cited newspapers, who also published data coming from WikiLeaks, and their service providers were not affected.

It seems then that the danger for the politicians who played a role in this case was identified in the model of information multicasting allowed by the Internet and the new tools, as they addressed all the threats to
subjects promoting or supporting such model. And in this case, the pressure seems to have reached quite easily and rapidly, at least in some measure, their target.

If information multicasting may really increase transparency beyond the point reachable with traditional models and augment the citizens’ consciousness and their demand for better government, the "Cablegate" case (one of the first of this genre) seems to demonstrate that such model can be impeded. As the new information multicasting module requires a few essential services, provided by subjects easily identifiable, parties interested in blocking information dissemination can limit their action to the agents (the service providers), even when the principal (the information provider) resists.

5. CONCLUSION

This paper aims to investigate the specific phenomenon of the service providers’ impact on the increased transparency fostered by the diffusion of data and information on the Internet, thereby allowing citizens to be informed on specific decisions made and actions taken by public administrations and governments. We assume that an increased transparency may in the end yield a positive effect on governments, as more informed citizens demand to be better governed.

The paper analyzes the "Cablegate" case, regarding the online publication by WikiLeaks of a huge amount of US diplomatic cables on November 2010, which provoked several reactions altering the behavior of most WikiLeaks' service providers. Regarding the communication flow of data and information among citizens and public organizations, we call the model promoted by WikiLeaks a "multicasting model". In this model, official data and information are provided to everyone by possibly several unofficial subjects. This model differs from the broadcasting model traditionally adopted by governments and public administrations. In the broadcasting model, data and information come out from few official sources, and are later diffused and commented by traditional media operators. The "multicasting model" is based on few essential services, mainly financial and technical.

To study the relationship between WikiLeaks and each service providers we adopted agency theory as a theoretical framework (Eisenhardt, 1989). We classified the service providers engaged in such process in a three-group taxonomy: financial operators, technical service providers, and social networks. We observed that a shift in the perceived risk coming out of a relationship between the principal (the information provider) and an agent (a service provider), reinforced by the relevant diversity of their goals, may lead the agents to suddenly interrupt the relationship, even when formalized with a contract, also without any violation of the terms by the principal.

We also observed that pressures and threats wielded by authorities on service providers, in order to increase the risk linked to such relationships, quite easily and quickly reach their purpose, even when the information provider tries to resist. In the "multicasting model" whoever wants to impede the diffusion of data, can then act against service providers in order to reach its aim. Notwithstanding the greater ease in publishing information to a vast audience, with respect to traditional press, it also seems much easier to interfere with the “multicasting model”.

As the WikiLeaks case shows, subjects like the service providers, involved in support activities and not directly interested in information diffusion, with their behavior may then foster or hamper transparency, potentially altering the quality of the public organization activity.

REFERENCES


